BELDEN
SENDING ALL THE RIGHT SIGNALS

Solution Guide

Market Dynamics Facing Process Automation

Process automation industries have revolutionized operations by digitizing information and processes bringing new opportunity to generate knowledge from data, resulting in increased levels of productivity, safety, and quality.

Industry 4.0 is transforming data into information by interconnecting automation systems, smart devices, and the business network. This has allowed us to harvest and analyze data allowing for agile decision making for predictive maintenance and capacity modeling, resulting in continuous productivity and efficiency gains.

Data Acquisition Requires Connectivity

Industry 4.0 is predicated on devices being connected to a network. Concern comes from connecting devices that have never been connected in the past. This exposes these once air-gapped or physically-isolated control networks to the world of cybersecurity.

These environments, inclusive of their safety instrumented systems, can now be a direct target of cyber-attacks. What's unique about process automation is that water/wastewater are considered critical infrastructure. This means the incapacity to operate or physical destruction of this infrastructure would have devastating impacts on the economy and/or public safety. **Protecting process automation systems from cyber-attacks has never been more important.**

Step One: **Visibility**

Having visibility of your automation environment is the first step to a cyber-secure network. Tripwire Industrial Visibility and Tripwire Log Center provide this visibility by:

- Understanding all the devices on your control network inclusive of remote networks for upstream (drilling), midstream (pipeline), downstream (refining), and offshore environments, who they are communicating with, and when their configurations change
- Correlating log events from multiple sources and writing rules to flag events of interest. For example, if a failed login is attempted 5 times on a critical device, Tripwire Log Center emails an automatic notification to the network manager

Step Two: **Protective Controls**

Once complete visibility has been achieved, the right protective controls to mitigate the risk or impact of cyber events can be put into place. Whether adopting a framework or guideline, such as IEC 62443, all industrial cybersecurity frameworks call for two basic, fundamental measures:

- **Network Segmentation:** Hirschmann EAGLE and Tofino Security appliances enable robust network segmentation (organizing networks into smaller segments and explicitly permitting communication required for the industrial application.)
- **Device Hardening:** Ensure all devices such as HMI's, engineering workstations, switches, routers, etc. are configured to industry cybersecurity frameworks, such as IEC 62443.

Step Three: **Continuous Monitoring**

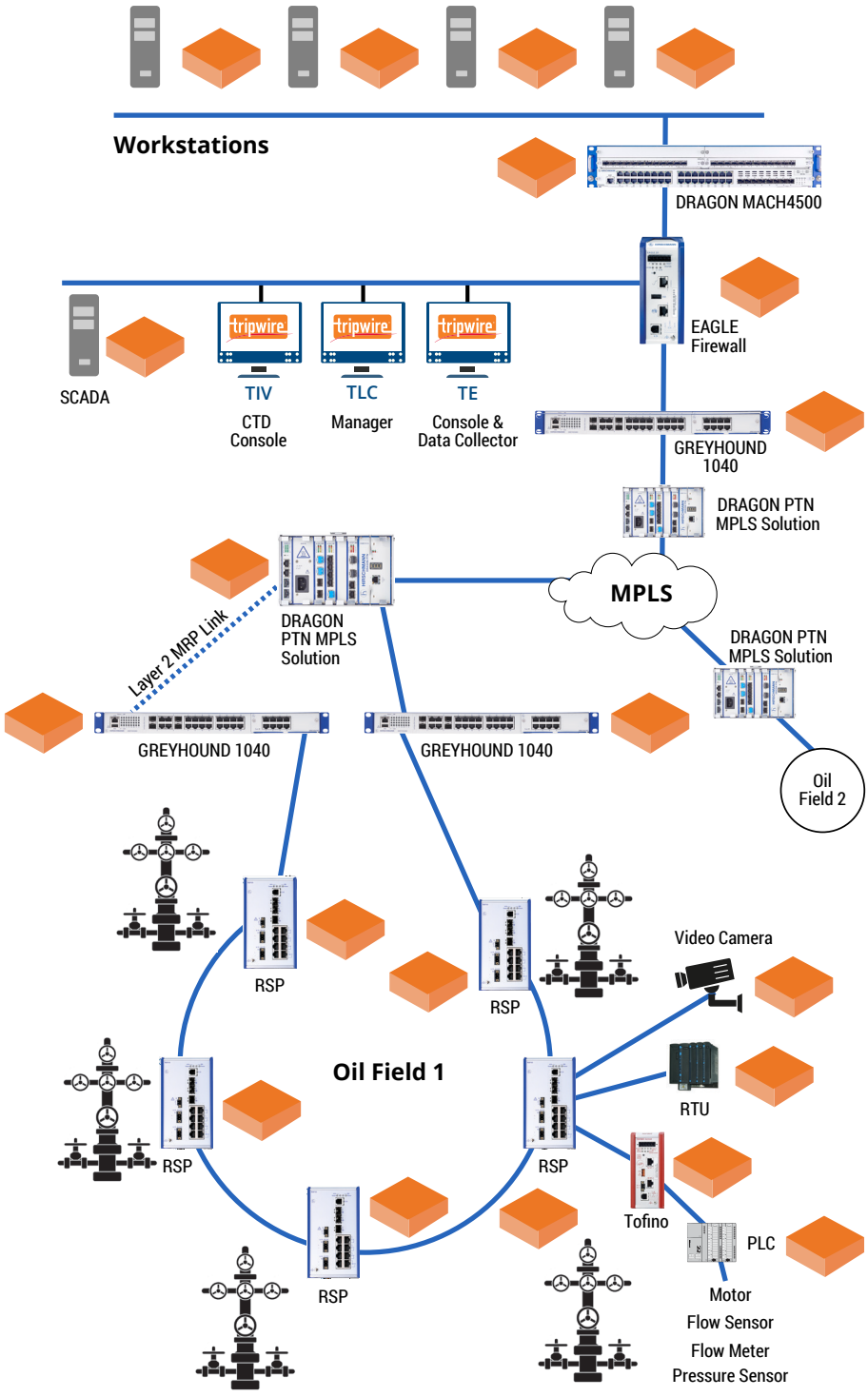
Once a foundation of visibility and protective controls has been established, you can begin to continuously monitor the environment for ongoing situational awareness to identify abnormal behavior to keep your process operational and avoid unplanned downtime. Tripwire solutions can enhance awareness by:

- **Understanding** when controller modes or configurations have been changed that do not map to authorized work orders
- **Discovering** if a rouge asset has been connected to the network and is propagating malware or making connections to external networks
- **Monitoring** engineering workstations to ensure correct configuration against internal build specifications or selected cybersecurity framework

Call your Belden or Tripwire sales representative to schedule a demonstration or visit our websites at www.belden.com and www.tripwire.com.

BELDEN
SENDING ALL THE RIGHT SIGNALS

Network Reference Architecture Example



TLC = Tripwire Log Center | TE = Tripwire Enterprise | TIV = Tripwire Industrial Visibility
Industrial visibility, protective controls and monitoring enabled through active and passive solutions: Tripwire Enterprise, Tripwire Log Center and Tripwire Industrial Visibility

Process Automation

Belden's solutions can:

- Provide complete asset inventory and industrial protocol communication
- Identify vulnerabilities to all assets
- Identify changes to controllers – configuration, mode and firmware
- Measure the configuration for HMI, SCADA, engineering workstations and network infrastructure to IEC 62443, American Water Works Association Process Control Guidance, and many others
- Provide visibility to log information from controllers, SCADA, HMI, engineering workstations and network infrastructure
- Provide network segmentation between plant and corporate IT, inter-zone/cell communication and enforce all industrial protocol communication to controllers

Customer Successes

- Petrochemical: Saved hundreds of man hours by automating manual configuration posture assessment of devices across 80 plants to mitigate the risk of malware propagation
- Water/Wastewater: Evaluated how their SCADA and HMI servers were configured as compared to the American Water Works Association Process Control Network recommendation

Belden
US 1-855-400-9071
EMEA +49 (0)7127 14 1809
APAC +65 6879 9800

Tripwire
US 1-503-276-7500
EMEA +44 (0) 16 2877 5850
APAC +65 6879 9839